



## Elevated Privileges Internet Restrictions

### Practice 8.2.4

Issue Date: 03/21/2011

Effective Date: 03/21/2011

1. Purpose

Decrease the damage possibilities of malware infections by prohibiting those with elevated privileges from surfing the Internet. Malware infections of devices used by those with elevated privileges pose much greater risk to broader and more severe negative ramifications.

2. Revision History

| Revision Date | Revision Number | Change Made | Reviser  |
|---------------|-----------------|-------------|----------|
| 03/21/2011    | 01              | Established | T. Stahl |

3. Persons, Groups, Systems Affected

All users with elevated privileges in Executive Branch domains

4. Responsibilities

Administrators – apply best practices to minimize the risk of and from malware infections. A second ID without elevated privileges should be used for non-technical support business and *de minimis* web navigation

5. Internet Block Settings

Internet web sites will be blocked for those with elevated privileges except for web sites “needed” for technical support. Sites permitted will be limited to those providing direct technical support through a web interface or software fixes/patches. Sites allowed will not include technical forums or magazines.

Submission of sites to be allowed for elevated user accounts, along with a brief justification, should be sent by a manager to the [IOTSecurityrequest@iot.in.gov](mailto:IOTSecurityrequest@iot.in.gov) mailbox. This is a separate process from the one used to approve sites for specific individuals.

6. Discipline

Bypassing or attempting to bypass these filtering exceptions shall result in discipline up to and including dismissal.